University of Oslo
INF3510 Information Security
Spring 2012
Workshop Questions and Answers

Lecture 7: User Authentication

Question 1

a. What is the limitation of user authentication for protection of communication?
b. What is a challenge-response authentication protocol, and what is its purpose?
c. Explain the steps of the HTTP digest user authentication protocol.

Answer

a. Two limiting elements of user authentication are
   • Does not guarantee user presence at the terminal after the authentication
   • Does not guarantee data received through the session originate from the user
b. A challenge-response protocol is an exchange of messages between two parties where one party (the verifier) challenges the other party (the applicant) to prove knowledge of a secret. The purpose of a challenge response-protocol is to prove to a remote party the knowledge of a secret without sending the secret to the remote party.
c. The HTTP Digest goes approximately as follows:
   i. Server sends a nonce (random number) to browser
   ii. Browser displays window with input fields for UserId and Password,
   iii. User fills in UserId and Password.
   iv. Browser computes the response: Digest = H(UserId, Password, nonce)
   v. Browser sends Digest to server
   vi. Server computes the same digest and compares with the received digest.

Question 2

Browse through the article by Richard Smith on the Strong Password Dilemma http://www.cryptosmith.com/password-sanity/dilemma and review the lecture notes on passwords.

a. Briefly describe the problems and limitations associated with reusable passwords.
b. Briefly explain the typical security policy requirement for password selection. You can look at the example Password Policy document at: http://www.sans.org/resources/policies/Password_Policy.doc or at UiO's requirements for acceptable and secure passwords at: http://www.uio.no/tjenester/it/brukernavn-passord/passord.html
c. In particular check what advice is given (if any) by the policy and requirements referred to under (b) regarding using the same or similar passwords for different services.
d. Why is it often recommended to memorize passwords, and not to write passwords down?
e. Assume that you don't agree with (d), suggest alternative methods for managing personal passwords, and discuss their security issues.

Answer

a. Some of the problems and limitations are:
   • Easy to share (intentionally or not) and forget.
   • Often easy to guess
   • Can be written down
   • Do not provide non-repudiation.
b. Refer to the final section “Forcing Functions and Mouse Pads” in the article of Richard Smith. Writing down a password may help the user in confidently choosing a good quality one. However, if they are written down passwords should be kept in a safe place (locked up or in a wallet) and not stuck to the computer monitor or under the mouse mat.
c. The password policy states that passwords should:
   • have sufficient minimum length, typically 8 (UiO recommends exactly 8 characters);
   • be easy to remember;
   • not be based on personal information such as names, telephone numbers, date of birth
   • not consist of dictionary words;
   • avoid repeated characters.
d. Memorized passwords can not be lost or stolen.
e. People accumulate more and more online accounts. It is too much to expect that they memorize a strong and different password for every account. Users must be able to write them down. The medium for writing down passwords should always be offline.

Question 3

a. Briefly define the concept of a biometric system.
b. A biometric system may operate in either verification mode or identification mode. Briefly explain the operation of both of these modes. State which of these modes is easier to implement and explain why.
c. A basic biometric system consists of four main modules. Briefly describe these modules.

Answer

a. A biometric system is an automated method of verifying or recognising a person based upon a physiological or behavioural characteristic
b. In verification mode the user claims an identity. A new biometric sample is captured and compared to the stored template corresponding to the user’s claimed identity. A decision is made on the closeness of the match – access is accepted or rejected. In identification mode the user does not claim an identity. A new biometric sample is captured and a search is conducted of the templates of all the users in the database for a match. Identification is more complex to implement since it requires n-to-1 matching instead of 1-to-1 matching required for verification.
c. The elements are
   - Sensor module: captures the biometric signal of an individual. An example is a fingerprint sensor that images the ridge and valley structure of a user’s finger.
   - Feature extraction module: processes the acquired biometric signal to extract a set of salient or discriminatory features. For example, the position and orientation of minutiae points (local ridge and valley singularities) in a fingerprint image are extracted in the feature extraction module of a fingerprint-based biometric system.
   - Matcher module: features captured during recognition are compared against the stored templates to generate matching scores.
   - System database module: used by the biometric system to store the biometric templates of the enrolled users.

Question 4

a. Any human physiological or behavioural characteristic can be used as a biometric characteristic as long as it satisfies four basic requirements. Briefly describe these four basic requirements.
b. For the practical implementation of a biometric system three additional requirements should also be considered. Briefly describe these three additional requirements.
c. Briefly describe the extent to which each of the following biometric types satisfies the characteristics and issues you described for parts (a) and (b).
   • Fingerprints
   • Facial recognition
   For background information, look at the article: "*An Introduction to Biometric Recognition*" http://www2.citer.wvu.edu/members/publications/files/RossBioIntro_CSVT2004.pdf

Answer

a. The requirements are:
   - Universality: each person should have the characteristic;
   - Distinctiveness: any two persons should be sufficiently different in terms of the characteristic;
   - Permanence: the characteristic should be sufficiently invariant (with respect to the matching criterion) over a period of time;
   - Collectability: the characteristic can be measured quantitatively.
b. The issues are
   - Performance: the achievable recognition accuracy and speed, the resources required to achieve the desired recognition accuracy and speed, the operational and environmental factors that affect the accuracy and speed;
   - Acceptability: the extent to which people are willing to accept the use of a particular biometric identifier (characteristic) in their daily lives;
   - Circumvention: how easily can the system be fooled using fraudulent methods.
c. Jain, Ross and Prabhakar (2004) give a table which includes the following extract. Here H, M, L stand for high, medium and low, respectively. In all cases H is the most desirable (for example, H for circumvention means that resistance to circumvention is high).

	Univer-sality	Unique-ness	Perma-nence	Collect-ability	Perfor-mance	Accept-ability	Cirum-vention
Facial rec.	H	L	M	H	L	H	L
Fingerprints	M	H	H	M	H	M	H

   - **Fingerprints:** A small proportion of people do not have suitable fingerprints for identification because of genetic, age, environment or occupation. Therefore universality is only medium. Fingerprints are practically unique and quite permanent. Fingerprint scanners are quite affordable and appear on many commodity devices today. Taking fingerprints is somewhat intrusive and often associated with criminal activity so is not as acceptable as some methods.
   - **Facial recognition:** This method is non-intrusive and scores well on universality and acceptability. There are different methods to obtain an accurate quantitative sample so collectability is good. Measurements can vary considerably with lighting and viewing angle which detracts from permanence. Moreover, facial measurements on their own provide a questionable basis for identification, so uniqueness and performance are rated low. This also affects circumvention, particularly if the subject does not cooperate (for example by presenting a different viewing angle).

Question 5

a. The response of a biometric matching system is the score *s* that quantifies the similarity between the input sample and the stored sample. Explain how the score *s* and the threshold *T* are used to determine mate pairs and non-mate pairs between the samples.
b. The threshold *T* should be tuned to provide the optimal balance between FAR (False Acceptance Rate) and FRR (False Rejection Rate). Explain roughly the principle for adjusting threshold *T* as a function of the costs associated with false accept and false reject.

Answer

a. Pairs of biometric samples generating score *s* where $s \geq T$ are inferred as mate pairs (i.e., belonging to the same person), and thus accept. Pairs of biometric samples generating score *s* where $s < T$ are inferred as non-mate pairs, and thus reject.
b. High *T* value is needed on case of high cost of false acept. Low *T* value is needed in case of high cost of false reject.

Question 6

Several national governments have specified national authentication frameworks. The Norwegian FANR "*Framework for Authentication and Non-Repudiation*" can be accessed at http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/eID_rammeverk_trykk.pdf
The Australian NeAF "*National e-Authentication Framework*" can be accessed at: http://www.finance.gov.au/e-government/security-and-authentication/docs/NeAF-framework.pdf

a. To what degree are the authentication assurance levels of FANR and NeAF compatible?
b. FANR does not explicitly focus in identity registration, whereas NeAF does. Give a possible explanation for why FANR does not focus on identity registration.
c. How many Authentication Assurance Levels (AAL) does NeAF specify and what are they called?
d. What does "Identity Registration Assurance Level 0" means in the NeAF terminology?
e. NeAF specifies the possibility of registering anonymous identities. Explain why it could be meaningful to have high authentication assurance level in a pseudonym identity?

Answer

a. NeAF specifies AAL 0 which FANR does not include. Therefore, NeAF AAL 0 and 1 would correspond to FANR level 1. The other levels are compatible.
b. In Norway the Person Register is considered a reliable source of registered identities, and is therefore not included in FANR.
c. NeAF specifies 5 different AALs (Authentication Assurance Levels: 0: No Assurance, 1: Minimal Assurance, 2: Low Assurance, 3: Moderate Assurance, 4: High Assurance
d. No registration
e. E.g. to provide high sensitivity service to anonymous persons for privacy protection purposes.